

Claims

1. A communication processing apparatus for executing
a communication process via a network, characterized in
5 that:

a communication process related to an
authentication process according to a predetermined
authentication method is performed in order to acquire
secret information permitted to be disclosed only to
10 devices in a local network corresponding to said
authentication method;

unique identification information of a
communication destination device in said communication
process is acquired by data processing at a network layer
15 or lower of an OSI reference model;

unique identification information of an
authentication partner device is acquired in an
authentication sequence of said authentication method as
data processing at an application layer of the OSI
20 reference model;

said acquired unique identification information
identification information of said communication
destination device is matched with said acquired unique
identification information of said authentication partner
25 device; and

in accordance with a passed or failed state of the
matching, a process is executed to judge whether said

authentication partner device is a device connected to a same local network as a local network to which a local device being a communication source device is connected.

5 2. The communication processing apparatus as claimed
in Claim 1, characterized that at least one of said
unique identification information received from said
communication destination device is received as processed
data generated by an encryption process or a hash value
10 generation process based on secret information shared
with said communication source device.

3. The communication processing apparatus as claimed
in Claim 1, characterized in that identification
15 information received from said communication destination
device is a node unique ID defined in IEEE 1394 standards.

4. The communication processing apparatus as claimed
in Claim 1, characterized in that:

20 said communication processing apparatus is
configured to receive, as identification information
received from said communication destination device,
identification information acquired by a PHY
communication unit of said communication destination
25 device and identification information acquired by a
network communication unit of said communication
destination device, and match a plurality of these

identification information.

5. The communication processing apparatus as claimed
in Claim 1, characterized in that identification
5 information received from said communication destination
device is a device address defined in communication
standards.

6. The communication processing apparatus as claimed
10 in Claim 1, characterized that said communication
processing apparatus is configured to receive, as
identification information received from said
communication destination device, a device address as a
source address of a packet transmitted from said
15 communication destination device, and a device address
stored in a packet by data processing at an application
level or data based on the device address, and match a
plurality of these device addresses.

20 7. A communication controlling method for executing a
communication process via a network, said method
characterized by comprising:

an identification information acquiring step of
acquiring unique identification information of a
25 communication destination device in a communication
process by data processing at a network layer or lower of
an OSI reference model, and acquiring unique

identification information of an authentication partner device in an authentication sequence of a predetermined authentication method as data processing at an application layer of the OSI reference model;

5 a matching processing step of performing a matching of said acquired unique identification information of said communication destination device with said acquired unique identification information of said authentication partner
10 device; and

 a judging step of judging, in accordance with a passed or failed state of the matching, whether said authentication partner device is a device connected to a same local network as a local network to which a local
15 device being a communication source device is connected.

8. The communication controlling method as claimed in Claim 7, characterized in that in said identification information acquiring step, at least one of said unique
20 identification information received from said communication destination device is received as processed data generated by an encryption process or a hash value generation process based on secret information shared with said communication source device.

25

9. The communication controlling method as claimed in Claim 7, characterized in that identification information

received from said communication destination device is a node unique ID defined in IEEE 1394 standards.

10. The communication controlling method as claimed in
5 Claim 7, characterized in that said identification
information acquiring step is a step of receiving, as
identification information received from said
communication destination device, identification
information acquired by a PHY communication unit of said
10 communication destination device and identification
information acquired by a network communication unit of
said communication destination device, and said matching
processing step matches a plurality of these
identification information.

15

11. The communication controlling method as claimed in
Claim 7, characterized in that identification information
received from said communication destination device is a
device address defined in communication standards.

20

12. The communication controlling method as claimed in
Claim 7, characterized in that:

said identification information acquiring step
receives, as identification information received from
25 said communication destination device, a device address
as a source address of a packet transmitted from the
communication destination device, and a device address

stored in a packet by data processing at the application level or data based on the device address, and

said matching processing step matches a plurality of these device addresses.

5

13. A computer program for executing a communication process via a network, said program characterized by comprising:

an identification information acquiring step of
10 acquiring unique identification information of a communication destination device in a communication process by data processing at a network layer or lower of an OSI reference model, and acquiring unique
identification information of an authentication partner
15 device in an authentication sequence of a predetermined authentication method as data processing at an application layer of the OSI reference model;

a matching processing step of performing a matching
of said acquired unique identification information
20 identification information of said communication destination device with said acquired unique identification information of said authentication partner device; and

a judging step of judging, in accordance with a
25 passed or failed state of said matching, whether said authentication partner device is a device connected to a same local network as a local network to which a local

device being a communication source device is connected.